STANDARD ADMINISTRATIVE PROCEDURE

29.01.03.M1.07 Information Resources – Change Management

Approved July 18, 2005
Revised February 24, 2009
Revised December 4, 2009
Revised August 14, 2013
Next scheduled review: August 14, 2018

Standard Administrative Procedure Statement

This SAP provides the components and steps for the appropriate management of changes to information resources.

Definitions

Confidential - Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Examples of "Confidential" data may include but are not limited to the following:

- Personally Identifiable Information, such as: a name in combination with Social Security number (SSN) and/or financial account numbers.
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Custodian - The person responsible for implementing owner-defined controls and access to an information resource. The custodian is responsible for the processing and storage of information and is normally a provider of services.

Change -

- Any implementation of new functionality;
- Any interruption of service;
- Any repair of existing functionality; or
- Any removal of existing functionality.

Mission Critical Information - Information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Owner of an Information Resource - An entity responsible for:

- a business function; and,
- determining controls and access to information resources supporting that business function.

Official Rule/Responsibilities/Process

---

1. GENERAL

   The information resource infrastructure at Texas A&M University is expanding. As the interdependency among information resources grows, the need for an effective change management process is essential.

   From time to time, information resources require a service disruption for planned upgrades, maintenance or fine-tuning. Additionally, such activities may result in unplanned service disruptions. Managing these changes is a critical part of providing a robust and valuable information resource infrastructure. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact to the user community.

   The goal of change management is to ensure that changes are controlled, implemented and documented in an orderly manner. This also helps to ensure that the intended purpose of the change is successfully accomplished and eliminates or minimizes any negative impact to the users of the resources as a result of the change. Proper application of change management also minimizes unwanted reductions in security and provides an accurate record of changes and associated supporting documentation that is useful when planning future changes.

2. APPLICABILITY

   This Standard Administrative Procedure (SAP) applies to multi-user systems storing or processing mission critical and/or confidential information. The degree to which change management procedures are employed is directly related to the risk and complexity of the change. The section entitled "Guidelines and Forms" provides guidance regarding the appropriate procedures for various risk/complexity levels.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP *29.01.03.M1.27 Exclusions from Required Risk Mitigation Measures*.

The intended audience is information resource owners and system administrators of University information resources that store or process mission critical and/or confidential information.

3. PROCEDURES

A consistent process is to be used for the implementation of information resource changes. The degree to which change management activities and processes are employed is dependent upon the projected inherent risk of the change (e.g., potential for unplanned disruption of service, corruption/loss of data, or disclosure of confidential information resulting from the change implementation) and the complexity of the information resources (e.g., number of users, interconnections with other systems, or number of components or subsystems).

Guidelines published at http://it.tamu.edu/Search.php?q=Change+Managment provide guidance for determining the level of change management procedures necessary. Where appropriate, the process should include: preparation, review/approval, notification, implementation, post-implementation review, and documentation.

3.1. Preparation may include:

3.1.1. Review of results of previously implemented changes to prevent repetitive mistakes or negative impacts.

3.1.2. Determination of the following:

1) the best time/date for implementation (to minimize the impact to users) and the length of time required;

2) the net impact to other systems or impact to normal operation during and following the change implementation (inherent risk); and,

3) the risk associated with the change implementation (to minimize the risk of disruption of service caused by the change).

3.1.3. Development of a back-out/rollback plan in the event that the change needs to be reversed and identification of a back-out/rollback window (the time period in which the decision to reverse the change can safely be made);

3.1.4. Confirmation that the changes will not negatively impact the overall system security.

3.1.5. Obtaining the concurrence of the information resource owner for implementation of the change.

3.2. Review/approval may include:

3.2.1. Determination of the level of control necessary based on inherent risk. Typically, the higher the risk the greater the level of control required. Controls include, but are not limited to, levels of approval, types of testing performed, length of review time, and consultation with subject matter experts.

3.2.2. Review of change-related details, including code review where appropriate, by the individual(s) responsible for approving the change or their designates.

3.2.3. Review of logs for previous change implementations.

3.2.4. Formal, documented approval or rejection of the change.

3.2.5. For changes involving code revision, review and approval shall be performed by someone other than the developer.

3.2.6. For emergencies, where this is not possible, establish a timely management review process.

3.3. Notification must be given to users in a timely manner, including relevant details that would not negatively impact the security of the information resource, such as time and date, nature of the change (e.g., projected net effect), and time needed for implementation. The method of notification should be appropriate to the environment and the user base, but may include email or an announcement posted on the web.

3.4. Implementation should be performed in the approved manner, with adequate separation of duties for tasks that are susceptible to fraudulent activity.

3.5. Post-implementation review may include:

3.5.1. Verification that the change occurred.

3.5.2. Testing of the system post-change.

3.5.3. Resolution of any problems, if possible.

3.5.4. Decision on whether to initiate back-out plan.

3.5.5. Analysis and of any issues or complications.

3.6. Documentation is performed post-implementation in order to provide a record of change (audit trail) that can be used in preparation for future changes or in future problem or incident handling. Documentation may include:

3.6.1. Date/time of change.

3.6.2. Duration or length of time required to implement the change.

3.6.3. Nature of the change (a brief description of the net effect, including the information resource(s) affected).

3.6.4. An indication of successful or unsuccessful completion of the change.

3.6.5. Identification of personnel involved in the change.

3.6.6. Updates to relevant operational documentation.

3.6.7. Any relevant documentation from the review & approval process.

3.6.8. Analysis and "lessons learned" (corrective/preventative actions) for changes that deviated unexpectedly from the plan, resulted in an unplanned disruption of service, corruption of data, or disclosure of confidential information.

Related Statutes, Policies, or Requirements

Supplements University SAP *29.01.03.M0.01, Security of Electronic Information Resources*

Texas A&M Information Security Control SA-3 *System Development Life Cycle*

Guidelines and Forms

Guidelines, forms and templates relating to Change Management are located on the Information Technology Risk Management site at http://it.tamu.edu/Search.php?q=Change+Managment.

Contact Office

CONTACT: Office of the Chief Information Security Officer

OFFICE OF RESPONSIBILITY: Vice President for Information Technology & Chief Information Officer